REMARKS

In response to the final office action mailed on July 22, 2005, Applicant requests reconsideration of the final rejection on the basis of the following remarks.

1. SECTION 103 REJECTION OF CLAIMS 18 AND 21

1.1 No motivation to combine the references

In responding to the first office action, Applicant argued that the Examiner had combined the references in hindsight. In the final office action, the Examiner excuses this hindsight reconstruction by citing an opinion rendered 34 years ago by a court that no longer exists. In particular, the Examiner quotes the CCPA as stating that "any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning" and that such [hindsight] reconstruction is proper "so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure."[1]

Applicant draws attention to more recent precedent that unequivocally affirms the impropriety of hindsight reconstruction. For example, in 1992, the Federal Circuit stated:

> It is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious. *In re Gorman*, 933 F.2d 982, 987, 18 USPQ2d 1885, 1888 (Fed. Cir. 1991). This court has previously stated that "[o]ne cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." (quoting *In re Fine*, 837 F.2d at 1075, 5 USPQ2d at 1600).[2]

More recently, the Federal Circuit stated that:

> "Our case law makes clear that the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references"[3]

As recently as four years ago, the Federal Circuit, in reaffirming its stance on the impropriety of hindsight reconstruction, stated that

> "[t]he genius of invention is often a combination of known elements which in hindsight seems preordained. To prevent hindsight invalidation of patent claims, the law requires some 'teaching suggestion, or reason'

---

[1] *Final Office Action*, paragraph 9, quoting *In re McLaughlin*, 443 F.2d 1392 (CCPA 1971).
[2] *In re Fritch*, 972 F.2d 1260, 1266 (Fed. Cir. 1992).
[3] *In re Dembiczak*, 175 F.3d 994 (Fed. Cir. 1999).

> to combine cited references."[4]

It is quite plain that the examiner must show that the motivation to combine the references existed *in the prior art*. As the Federal Circuit stated in *Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 934, 15 USPQ2d 1321, 1323 (Fed. Cir. 1990):

> It is insufficient that the prior art disclosed the components of the patented device, either separately or used in other combinations; there must be some teaching, suggestion, or incentive to make the combination made by the inventor.

In the present case, the Examiner makes the following assertions to support the proposition that a motivation to combine *Denning* and *Thomson* existed as of June 20, 1996:

(a) encryption was known in 1996;

(b) encrypting data has *always* been desirable because encryption makes the data more secure, and

(c) "'enhancing security' is commensurate with the broad limitations of the claimed invention."[5]

With regard to (c), it is unclear how this statement shows that the *prior art* teaches a motivation to combine *Denning* and *Thomson*. If anything, (c) appears to be an admission that the motivation to combine *Denning* and *Thomson* came from Applicant's disclosure, i.e. "the broad limitations of [Applicant's] claimed invention," rather than the prior art.

Assertions (a) and (b) are so nebulous that they would render unpatentable *any* claimed subject matter that involves data encryption. Since patents involving data encryption exist, statements (a) and (b) cannot possibly provide a reasoned basis for combining *Denning* and *Thomson*.

Applicant also calls into question the accuracy of statement (b). In fact, encrypting data is not *always* desirable. After all, as of June 20, 1996, it was also known that at some point, encrypted data would need to be decrypted, and that such decryption would introduce latency.

---

[4] *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339 (Fed. Cir. 2001).
[5] *Final Office Action*, paragraph 9.

Moreover, if statement (b) accurately reflects reality as of the June 20, 1996 priority date, it is difficult to explain why at that time, people routinely mailed sensitive documents in sealed envelopes without bothering to encrypt them. It is also difficult to explain why, at that time, anyone would have exchanged e-mails containing sensitive information, particularly given the availability of e-mail encryption software.

Statement (b) is inaccurate because it neglects to consider the tradeoff between data security and data accessibility. An inaccurate factual statement, such as (b), cannot establish the existence of a motivation to combine *Denning* and *Thomson* as of the priority date.

In fact, it would have made no sense to combine *Thomson* and *Denning*. After all, *Thomson* had already disclosed a way to protect selected portions of a database from unauthorized access, while avoiding the complexity and overhead associated with encryption. There would have been no plausible motivation for complicating *Thomson*'s simple and elegant solution to the problem of unauthorized access to portions of the database by somehow incorporating into it the encryption scheme of *Denning*.

Moreover, *Denning* preceded *Thomson* by well over a decade. Had the combination of *Denning* and *Thomson* been as desirable as the Examiner suggests, it is difficult to explain why *Thomson* himself did not make the combination.

1.2 Proposed modification renders *Thomson* unsatisfactory for its intended purpose

A proposed modification is improper if it would render the prior art unsatisfactory for its intended purpose.[6]

In this case, the intended purpose of *Thomson* is to provide an extremely simple way to permit certain users to access only selected rows of a database:

> "It is desirable to improve the ease of effecting security, in particular row security, with a minimum amount of effort and time to implement"[7]

---

[6] MPEP 2143.01, referring to *In re Gordon*, 733 F.2d 900 (Fed. Cir. 1984).
[7] *Thomson et al.*, U.S. Patent No. 5,751,949, col. 2, lines 9-12.

After describing his solution for carrying out this intended purpose, *Thomson* draws attention to one of its particular advantages, namely that "[n]o program changes are required in the relational database software itself, but improved and simplified security is nevertheless available"[8]

The Examiner proposes to complicate matters considerably by imposing upon *Thomson* the additional burden of encrypting selected fields and having to somehow manage the keys associated with those fields. As pointed out above, the intended purpose of *Thomson* is to provide "row security with a minimum amount of effort and time to implement." At the very least, the proposed modification would require some modification to the relational database software itself, which would now need to distinguish between clear text and encrypted fields, to search for the key that corresponds to an encrypted field, and to then carry out the decryption. This proposed modification is undesirable because it would obviate the expressly-stated advantage of *Thompson*'s solution.

1.3 A prima facie case of obviousness has not been established

To establish prima facie obviousness, "either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references."[9]

In this case, the Examiner's "convincing line of reasoning" rests on two observations: (1) encryption was known; and (2) encryption was known to be desirable because encrypted data is more secure. This pair of rudimentary observations hardly rises to the level of a "convincing line of reasoning" as required by section 103.

The inadequacy of this line of reasoning is readily apparent by observing that the converse point of view is equally plausible. After all, it is certainly true that at the time of the invention: (1) encryption was known; and (2) encryption was known to add latency and complexity, thereby rendering it *undesirable*. Moreover, it was also known at the time that there

---

[8] *Thomson*, col. 6, lines 12-13.
[9] MPEP 2142, referring to *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985).

existed *other* ways to protect data *without* the complexity of encryption. In fact, the Examiner has already found one such way: *Thomson*.

The Examiner apparently subscribes to the idea that the more ways one protects data, the better. In the Examiner's view, if data is already protected once, it obviously should be protected twice. This is not "a convincing line of reasoning." It is merely an unthinking reflex that completely neglects the costs of security, both in latency and complexity.

In view of the absence of any reasoned basis for making the proposed combination of references. Applicant requests reconsideration and withdrawal of the second 103 rejection of claim 18.

Claim 56 includes limitations similar to claim 18. Accordingly, claim 56 is patentable for at least the reasons discussed above in connection with claim 18.

Claims dependent on claims 18 and 56 all contain the limitations of their respective parent claims, and are allowable for at least the same reasons.

For reasons set forth above, Applicant requests reconsideration and withdrawal of the section 103 rejection of claims 18 and 56, and all claims dependent thereon.

2. SECTION 103 REJECTION OF CLAIMS 41, 48, 79, 86

2.1 Inherency has not been demonstrated

In responding to the office action, Applicant drew attention to the absence of any express disclosure in *Denning* and *Thomson* of storing cryptographic information outside the table. In the final office action, the Examiner agrees that no express disclosure exists, but then suggests that such disclosure is nevertheless implied. The Examiner's position is based on the notion that because the contents of the table are either encrypted or non-sensitive, it would make no sense to store the key in the table. Therefore, a disclosure of storing the key separately from the table is inherent in the disclosure of *Denning*.

A reference inherently discloses a feature if the existence of that feature necessarily follows from the disclosure. However, if the absence of the feature is also consistent with the

disclosure, then the reference fails to inherently disclose the feature. This statement of the law of inherency is articulated in MPEP 2112:

> "[t]he fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic"

as well as by the Board of Appeals:

> "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic *necessarily* flows from the teachings of the applied prior art"[10]

and again, nine years later, by the Federal Circuit itself:

> To establish inherency, the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." Continental Can Co. v. Monsanto Co., 948 F.2d 1264, 1268, 20 U.S.P.Q.2d 1746, 1749 (Fed.Cir.1991). "Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." Id. at 1269, 948 F.2d 1264, 20 U.S.P.Q.2d at 1749 (quoting In re Oelrich, 666 F.2d 578, 581, 212 U.S.P.Q. 323, 326 (C.C.P.A.1981)).[11]

In fact, it would not be at all unreasonable for *Denning* to store a key in a table. For example, data in a column of a table can be encrypted with a user-specific key that is stored, after having been encrypted under a common key, with the data in that column.

Because of the foregoing counter-example, *Denning* fails to inherently disclose storage of cryptographic information outside the table.

For reasons set forth above, Applicant requests reconsideration and withdrawal of the section 103 rejection of claims 41, 48, 79, 86, and all claims dependent thereon.

3. SECTION 103 REJECTION OF CLAIMS 32, 44, 51, 69, 82, 89

3.1 Proposed combination fails to disclose each limitation of the claim

The Examiner draws particular attention to column 7, lines 41-50 of *Abraham* to support the proposition that the combination of *Denning*, *Thomson*, and *Abraham* discloses storing, separate from the table, encrypted information for controlling access to information in that table.

---

[10] *Ex parte Levy*, 17 USPQ 2d 1461, 1464 (Bd. Pat. App. & Inter. 1990)[emphasis in original].
[11] *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999).

Applicant draws particular attention to the text at column 7, lines 45-48 which states:

> Keys are stored on PC disk memory in encrypted form, encrypted under the master key of one of the security devices. [sic] cryptographic adapter **29**, card reader **17**, or IC card **19**.[12]

Abraham thus teaches storing encrypted keys on PC disk memory. This is not the same as teaching that encrypted keys are stored separately from the table, particularly since a table would likely be stored in PC disk memory as well. *Abraham* is, at best, inconclusive. It is silent as to whether the encrypted key is stored with a table or separately from a table.

The foregoing passage also suggests that *Abraham* stores, in a security device, a master key that is used to encrypt another key, which is ultimately stored in disk memory. However, this master key does not appear to be encrypted.

The Examiner suggests that the encrypted key must be stored separately from the table for reasons set forth in paragraph 9 of the final office action. In response, Applicant draws attention again to the counter-example described above in connection with the discussion of inherency.

Applicant submits therefore that the section 103 rejection of the foregoing claims is improper because the proposed combination fails to disclose each and every limitation of the claimed invention. Applicant also maintains that the section 103 rejection is improper for the reasons discussed in connection with claim 18.

SUMMARY

Now pending in this application are claims 18-54 and 56-92, of which claims 18, 41, 48, 56, 74, and 86 are independent. No additional fees are believed to be due in connection with this filing of this request for reconsideration. However, to the extent fees are due, or if a refund is forthcoming, please adjust our deposit account 06-1050 referring to Attorney Docket No. "17299-008002."

---

[12] *Abraham et al.*, U.S. Patent No. 5,148,481, col. 7, lines 45-48.

Respectfully submitted,

Date: 9-21-05

Faustino A. Lichauco
Reg. No. 41,942

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906
21171015.doc